UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

BRIAN HOLOVATY, on behalf of himself and on behalf of all other similarly situated individuals,

Plaintiff,

v.

ILLINOIS BONE & JOINT INSTITUTE, LLC,

Defendant.

Case No. 1:24-cv-08499

JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiff Brian Holovaty ("Plaintiff"), individually and on behalf of all other similarly situated individuals (the "Class" or "Class Members," as defined below), by and through his undersigned counsel, files this Class Action Complaint against Illinois Bone & Joint Institute, LLC ("IBJI" or "Defendant") and alleges the following based on personal knowledge of facts, upon information and belief, and based on the investigation of his counsel as to all other matters.

I. INTRODUCTION

1. Plaintiff brings this class action lawsuit against IBJI for its negligent failure to protect and safeguard Plaintiff's and the Class's highly sensitive personally identifiable information ("PII") and protected health information ("PHI"). As a result of IBJI's negligence and insufficient data security, cybercriminals easily infiltrated Defendant's

inadequately protected computer systems and ***stole*** the PII and PHI of Plaintiff and the Class (approximately **182,670 individuals**) (the "Data Breach" or "Breach").[1] Now, Plaintiff's and the Class's PII and PHI is in the hands of cybercriminals who will undoubtedly use their PII for nefarious purposes for the rest of their lives.

2. According to IBJI, on July 4, 2024, IBJI detected unauthorized access to certain computer systems on its network.[2]

3. After an investigation, Defendant files were copied, or in other words, stolen, from its network.[3]

4. The Private Information stolen in the Data Breach included highly sensitive private information such as: names, addresses, dates of birth, Social Security numbers, diagnosis and treatment information, and health insurance/claims information (collectively, "Private Information").[4]

5. IBJI confirmed after a forensic investigation that an unauthorized third party accessed the IBJI network between May 30, 2024, and July 4, 2024, and acquired certain files during this period.

6. Defendant acquired, collected, and stored Plaintiff's and Class Members' Private Information in connection with the medical services it provided. Therefore, at all relevant times, Defendant knew or should have known that Plaintiff's and Class Member's

[1] https://www.hipaajournal.com/illinois-bone-joint-institute-hacking-incident-affects-almost-183000-patients/.
[2] *Id.*
[3] *Id.*
[4] *Id.*

sensitive data, including their highly confidential Private Information would be stored on Defendant's networks.

7. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, Defendant assumed legal and equitable duties to Plaintiff and the Class. These duties arose from state and federal statutes and regulations as well as common law principles.

8. Defendant disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly and/or negligently failing to take and implement adequate and reasonable measures to ensure that Plaintiff's and Class Members' Private Information was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data and failing to follow applicable, required and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As a result, the Private Information of Plaintiff and Class Members was compromised through disclosure to an unknown and unauthorized third party—an undoubtedly nefarious third party that seeks to profit off this disclosure by defrauding Plaintiff and Class Members in the future.

9. Due to IBJI's negligent failure to secure and protect Plaintiff's and Class Members' Private Information, cybercriminals have stolen and obtained everything they need to commit identity theft and wreak havoc on the financial and personal lives of millions of individuals.

10. Now, and for the rest of their lives, Plaintiff and the Class Members will have to deal with the danger of identity thieves possessing and misusing their Private

Information. Even those Class Members who have yet to experience identity theft will have to spend time responding to the Data Breach and are at an immediate and heightened risk of all manners of identity theft as a direct and proximate result of the Data Breach.

11. Plaintiff and Class Members have incurred and will continue to incur damages in the form of, among other things, identity theft, attempted identity theft, lost time and expenses mitigating harms, increased risk of harm, damaged credit, diminution of the value of their Private Information, loss of privacy, and additional damages as described below.

12. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they are entitled to injunctive and other equitable relief.

13. Plaintiff brings this action individually and on behalf of the Class, seeking compensatory damages, punitive damages, nominal damages, restitution, injunctive and declaratory relief, reasonable attorneys' fees and costs, and all other remedies this Court deems just and proper.

II. THE PARTIES

14. **Plaintiff Brian Holovaty** is an individual domiciled in Des Plaines, IL. Plaintiff received a Notice of Data Breach Letter from IBJI dated August 30, 2024, notifying him that his name, address, date of birth, Social Security number, medical treatment or diagnosis information, and/or health insurance or claims information was compromised in the Data Breach.[5]

[5] Ex. 1 (Notice of Data Breach Letter).

15. Defendant **IBJI** is an Illinois Limited Liability Company with members and managers located in this District. IBJI's principal address is 900 Rand Rd., STE 300, Des Plaines, IL 60016-2359. IBJI's registered agent is Charmina Zigmond, located at the same address as its principal address.

III. JURISDICTION AND VENUE

16. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. §1332(d). The amount in controversy exceeds the sum of $5,000,000 exclusive of interest and costs, there are more than one hundred putative Class Members, and minimal diversity exists because many putative Class Members are citizens of a different state than Defendant.

17. Further, federal jurisdiction is proper because Defendant serves northern Illinois and northwest Indiana.[6] Defendant also sent Notice of Data Breach Letters to victims domiciled in Massachusetts, Vermont, and Texas, indicating federal jurisdiction is proper.

18. This Court has personal jurisdiction over Defendant because Defendant is a Illinois domestic limited liability company; has its principal place of business in this District; has members or managers domiciled in this District, conducts substantial business in this District through its headquarters, offices, and affiliates; engaged in the conduct at issue here in this District; and/or otherwise has substantial contacts with this District and purposely availed itself to the Courts in this District

[6] https://www.ibji.com/about-us/.

19. Venue is proper in this District under 28 U.S.C. §§ 1391(a)(2), 1391(b)(2), and 1391(c)(2) as a substantial part of the events giving rise to the claims emanated from activities within this District.

IV. FACTUAL ALLEGATIONS

A. Defendant's Collection of Plaintiff's and the Class's Private Information.

20. "Founded in 1991, IBJI is the largest orthopedic group practice in Illinois. With more than 150 physicians in every orthopedic specialty, IBJI offers care for children and adults from some of the most accomplished and respected orthopedists in the country."[7]

21. IBJI offers a full range of orthopedic care, including advanced MRI imaging, pain management, non-surgical and surgical treatment plans, rheumatology, physical therapy, occupational therapy, wellness and sports training.[8]

22. As part of the medical services Defendant provides, it is entrusted with and obligated to safeguard and protect the Private Information of Plaintiff and the Class in accordance with all applicable laws and industry standards.

23. Indeed, Defendant made promises and representations to its patients, including Plaintiff and Class Members, that the Private Information it collected from them would be kept safe, confidential, that the privacy of that information would be maintained.

24. Specifically, Defendant provides on its website: "IBJI takes patient confidentiality of outmost seriousness and we are required by the State of Illinois and

[7] *Id.*
[8] *Id.*

Federal law to maintain the privacy of your protected health information (PHI)."[9]

25. However, the Data Breach makes it clear that IBJI does not take patient confidentiality seriously nor does it follow state or federal law to protect Private Information.

26. Plaintiff and the Class Members have taken reasonable steps to maintain the confidentiality of their Private Information. Plaintiff and Class Members relied on the sophistication of Defendant to keep their Private Information confidential and securely maintained, to use this information for necessary purposes only, and to make only authorized disclosures of this information. Plaintiff and Class Members value the confidentiality of their Private Information and demand security to safeguard their Private Information.

27. Defendant had a duty to adopt reasonable measures to protect the Private Information of Plaintiff and Class Members from involuntary disclosure to third parties. Defendant has a legal duty to keep its patients' Private Information safe and confidential.

28. Defendant had obligations created by FTC Act, HIPAA, contract, industry standards, and representations made to Plaintiff and Class Members, to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

29. Defendant derived a substantial economic benefit from collecting Plaintiff's and Class Members' Private Information. Without the required submission of Private Information, Defendant could not perform the medical services it provides and obtain

[9] https://www.ibji.com/patient-resources/privacy-non-discrimination-policy/.

revenue.

30. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' Private Information from disclosure.

31. However, Defendant failed to take this responsibility seriously and failed to protect Plaintiff's and the Class's Private Information from unauthorized access, resulting in a massive and preventable data breach.

B. Defendant's Massive and Preventable Data Breach.

32. On July 4, 2024, IBJI detected unauthorized access to certain computer systems on the IBJI network.[10]

33. Afterwards, IBJI initiated an investigation and determined that an "unauthorized third party ***accessed*** the IBJI network between May 30, 2024, and July 4, 2024, and ***acquired*** certain files during this period."[11]

34. In other words, cybercriminals has unfettered access to Plaintiff's and the Class's Private Information for weeks and as a result, cybercriminals stole their Private Information.[12]

35. "IBJI determined that the systems in scope may contain personal information for certain individuals, including, depending on the individual, their name, address, date of

[10] https://www.ibji.com/data-security-incident/.
[11] *Id.* (emphasis added).
[12] *Id.*

birth, Social Security number, medical treatment or diagnosis information, and/or health insurance or claims information."[13]

36. IBJI sent written notification of the Data Breach ("Notice of Data Breach Letters") in or around August 30, 2024—months after the Breach occurred.[14]

37. The Notice Letter IBJI sent to victims of the Data Breach amounts to no real disclosure at all, as it fails to inform, with any degree of specificity, Plaintiff and Class Members of the Data Breach's critical facts such why the Data Breach went unnoticed for so long, why it took IBJI so long to notify affected individuals of the Breach, and who the perpetrator of the Data Breach is and if they have been caught. Without these details, Plaintiff's and Class Members' ability to mitigate the harms resulting from the Data Breach is severely diminished.

38. Furthermore, Defendant inexplicably delayed giving notice of the Data Breach to Plaintiff and the Class for weeks, giving cybercriminals a head starts in misusing and selling Plaintiff's and the Class's Private Information.

39. It is clear IBJI expects victims of the Data Breach to experience fraud and identity theft resulting from the Data Breach because IBJI states the following on its website:[15]

> As a precautionary measure, individuals should remain vigilant to protect against potential fraud and/or identity theft by, among other things, reviewing their account statements and monitoring credit reports closely. If individuals detect any suspicious activity on an account, they should promptly notify the financial institution or company with which the account

[13] *Id.*
[14] *See* Ex. 1.
[15] https://www.ibji.com/data-security-incident/.

> is maintained. They should also promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities, including the police and their state's attorney general. Notified individuals may also wish to review the tips provided by the Federal Trade Commission ("FTC") on fraud alerts, security/credit freezes and steps that they can take to avoid identity theft. For more information and to contact the FTC, please visit www.ftc.gov/idtheft or call 1-877-ID-THEFT (1-877-438-4338). Notified individuals may also contact the FTC at: Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

40. IBJI instructs victims of the Data Breach to place a fraud alert on their credit file, consider placing a security freeze on their credit file, and obtain a free credit report.[16] These are suggestions IBJI need not make if there were not an imminent risk of fraud and identity theft.

41. After receiving the Notice Letters, it is reasonable for recipients, including Plaintiff and Class Members, to believe that the risk of future harm (including identity theft) is substantial and imminent, and that it its necessary for them to take steps to mitigate that substantial risk of impending and future harm.

42. Defendant made a token gesture of a mere twelve (12) months of credit monitoring services to Plaintiff and the Class—an offer it need not have provided absent any threat to Plaintiff and the Class.[17] However, this offer is woefully inadequate considering Plaintiff and Class Members will be at a continued risk of fraud and identity theft for the rest of their lives. This gesture does not and will not fully protect Plaintiff and the Class from cybercriminals and is largely ineffective against protecting data after it has been stolen. Cybercriminals are fully aware of the well-publicized preventative measures

[16] *Id.*
[17] Ex. 1.

taken by entities after data breaches such as that which happened here and will, therefore, oftentimes hold onto the stolen data and not use it until after the complimentary service is no longer active, and long after victim concerns and preventative steps have diminished. There would be no need to provide credit monitoring services if Plaintiff and the Class were not at an imminent risk of harm due to the Data Breach.

43. It is apparent that the unauthorized third-party cybercriminals intentionally targeted and gained access to Plaintiff's and the Class's Private Information with the intent of engaging in misuse of the Private Information, including marketing and selling Plaintiff's and Class Members' Private Information to fraudsters as that is the *modus operandi* of data thieves.

44. Ransomware attacks are entirely preventable and should have been prevented by IBJI.

45. The following methods and controls can prevent ransomware attacks:

- **Microsegmentation**. By strictly limiting access to individual IT assets or small subsets of a network, software-defined microsegmentation can prevent the kind of lateral movement that is essential to ransomware attacks.
- **Security awareness training**. Educating employees is a critical part of preventing ransomware. Awareness training should include best practices for security hygiene as well as ways to recognize phishing emails and other common techniques for distributing ransomware.
- **Encryption**. Through encryption, organizations can prevent ransomware attackers from stealing and exposing sensitive data.
- **Strong identity and access control**. By implementing strong passwords and techniques like multifactor authentication, organizations can severely limit who can view or modify data, reducing the risk or the scope of a [] ransomware infection.
- **Backups**. Regular data backups allow organizations to recover quickly from a ransomware infection without having to pay a ransom or

permanently losing files. Backups must be stored in a secure location that is not connected to computers or the network, to prevent these storage locations from being infected.

- **Optimal patching cadence**. Regularly installing updates and security patches can help address the vulnerabilities in hardware, applications, and APIs that attackers may otherwise take advantage of.
- **Continuous monitorin**g. Network administrators should continuously monitor incoming and outgoing traffic to search for unusual patterns that may indicate a ransomware affection or other types of cyberattacks.
- **Endpoint security**. Endpoint security services provide protection at the device level to recognize and block attacks.
- **Secure cloud services**. When choosing cloud service providers, organizations must ensure that security teams understand the shared responsibility model for security that's involved in many cloud services, and ensure that providers comply with recognized standards and quality frameworks such as PCI DSS or the FedRAMP certification.
- **Data leak protection (DLP)**. DLP solutions enable granular classification of data based on sensitivity and can alert security teams in real time when potential ransomware incidents or data exfiltration are occurring.[18]

46. According to information and belief, IBJI did not have any of the above precautions in place prior to the Data Breach. Such precautions would have prevented the Data Breach.

47. In fact, IBJI admits it did not have proper data security measures in place, because it states the following on its website:[19]

> IBJI is committed to maintaining the privacy and security of the information entrusted to it and apologizes for any inconvenience this incident might cause. IBJI has taken, and is taking, additional steps to help reduce the likelihood of a similar event from happening in the future, including enhancing its technical security measures. Individuals seeking additional information may call a confidential, toll-free inquiry line at 866-574-0969 from 8:00 a.m. – 8:00 p.m. Central, Monday through Friday, excluding major U.S. holidays.

[18] *Id.*
[19] https://www.ibji.com/data-security-incident/.

48. IBJI should have implemented these enhanced technical security measures prior to the Data Breach to prevent the Data Breach from occurring.

49. IBJI did not use reasonable security procedures and practices appropriate to protect the sensitive information it was maintaining for Plaintiff and Class Members, such as encrypting the information or deleting it when it is no longer needed, which resulted in the access and exfiltration of Plaintiff's and the Class's Private Information.

50. The perpetrator of the Data Breach accessed and acquired files in Defendant's computer systems containing unencrypted Private Information of Plaintiff and Class Members, including their names, dates of birth, Social Security numbers, PHI, and other sensitive information.

51. Upon information and belief, the unauthorized third-party cybercriminal(s) gained access to the Private Information and engaged in (and will continue to engage in) misuse of the Private Information, including marketing and selling Plaintiff's and Class Members' Private Information on the dark web.

52. Plaintiff believes that his Private Information and that of Class Members was or will be sold on the dark web, as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type.

53. Plaintiff and Class Members' Private Information was provided to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

54. Accordingly, Defendant had obligations created by HIPAA, reasonable

industry standards, common law, statutory law, and its own assurances and representations to keep Plaintiff's and Class Members' Private Information confidential and to protect such Private Information from unauthorized access.

55. Nevertheless, Defendant failed to spend sufficient resources on preventing external access, detecting outside infiltration, and training their employees to identify threats and defend against them.

56. The stolen Private Information at issue has great value to the hackers, due to the large number of individuals affected and the fact that health insurance information and Social Security numbers were part of the data that was compromised.

C. Plaintiff's Individual Experience.

Plaintiff Holovaty's Experience

57. Plaintiff Holovaty received a Notice of Data Breach Letter from Defendant dated August 30, 2024, informing his that his Private Information was compromised in the Data Breach.[20]

58. Defendant was in possession of Plaintiff Holovaty's Private Information before, during, and after the Data Breach.

59. Because of the Data Breach, Plaintiff Holovaty's highly confidential Private Information is in the hands of cybercriminals. As such, Plaintiff Holovaty and the Class are at an imminent risk of identity theft and fraud.

60. As a result of the Data Breach, Plaintiff Holovaty has already expended hours

[20] Ex. 1.

of his time and has suffered loss of productivity from taking time to address and attempt to ameliorate, mitigate, and address the future consequences of the Data Breach, including investigating the Data Breach, investigating how best to ensure that he is protected from identity theft, and reviewing account statements and other information. Plaintiff Holovaty has been securing all of his accounts when he has time in his schedule and has received an abundance of scam text messages he attributes to the Data Breach.

61. Plaintiff Holovaty places significant value in the security of his Private Information and does not readily disclose it. Plaintiff Holovaty has never knowingly transmitted unencrypted Private Information over the internet or any other unsecured source.

62. Plaintiff Holovaty has been and will continue to be at a heightened and substantial risk of future identity theft and its attendant damages for years to come. Such a risk is certainly real and impending, and is not speculative, given the highly sensitive nature of the Private Information compromised by the Data Breach. Indeed, Defendant acknowledged the increased risk of future harm Plaintiff Holovaty, and the Class now face by offering complimentary credit monitoring services to Plaintiff Holovaty and the Class.

63. Knowing that thieves intentionally targeted and stole his Private Information and knowing that his Private Information is in the hands of cybercriminals has caused Plaintiff Holovaty great anxiety beyond mere worry. Specifically, Plaintiff Holovaty has lost hours of sleep, is in a constant state of stress, is very frustrated, and is in a state of persistent worry now that his Private Information has been stolen.

64. Plaintiff Holovaty has a continuing interest in ensuring that his Private

Information, which, upon information and belief, remains in the possession of Defendant, is protected, and safeguarded from future data breaches. Absent Court intervention, Plaintiff's and the Class's Private Information will be wholly unprotected and at-risk of future data breaches.

65. Plaintiff Holovaty has suffered injuries directly and proximately caused by the Data Breach, including: (i) theft of his valuable Private Information; (ii) invasion of privacy and the imminent and certain impending injury flowing from anticipated fraud and identity theft posed by his Private Information being placed in the hands of cybercriminals; (iii) damages to and diminution in value of his Private Information that was entrusted to Defendant for the sole purpose of obtaining services with the understanding that Defendant would safeguard this information against disclosure; (iv) loss of the benefit of the bargain with Defendant to provide adequate and reasonable data security—*i.e.*, the difference in value between what Plaintiff Holovaty should have received from Defendant and Defendant's defective and deficient performance of that obligation by failing to provide reasonable and adequate data security and failing to protect his Private Information; and (v) continued risk to his Private Information, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information that was entrusted to Defendant.

D. Defendant had an Obligation to Protect Private Information Under the Law and the Applicable Standard of Care.

66. Upon information and belief, Defendant is covered by HIPAA (45 C.F.R. § 160.102). As such, it is required to comply with the HIPAA Privacy Rule and Security

Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

67. HIPAA's Privacy Rule or *Security Standards for the Protection of Electronic Protected Health Information* establishes a national set of security standards for protecting health information, including health information that is kept or transferred in electronic form.

68. HIPAA requires Defendant to "comply with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302.

69. "Electronic protected health information" is "individually identifiable health information … that is (i) transmitted by electronic media; maintained in electronic media." 45 C.F.R. § 160.103.

70. HIPAA's Security Rule requires Defendant to do the following:

a. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits;

b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and

d. Ensure compliance by their workforce.

101. HIPAA also requires Defendant to "review and modify the security measures implemented … as needed to continue provision of reasonable and appropriate protection of electronic protected health information." 45 C.F.R. § 164.306(e).

102. Additionally, HIPAA requires Defendant to "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1).

103. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, further requires Defendant to provide notice of the Data Breach to each affected individual "without unreasonable delay and in no case later than 60 days following discovery of the breach."

104. Defendant did not comply with the HIPAA Breach Notification Rule.

105. Defendant was also prohibited by the Federal Trade Commission Act (the "FTC Act") (15 U.S.C. § 45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission (the "FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

106. Defendant is further required by various states' laws and regulations to protect Plaintiff's and Class Members' Private Information.

107. Defendant owed a duty to Plaintiff and the Class to design, maintain, and test its computer and email systems to ensure that the Private Information in its possession was adequately secured and protected.

108. Defendant owed a duty to Plaintiff and the Class to create and implement reasonable data security practices and procedures to protect the Private Information in its possession, including adequately training its employees (and others who accessed Private Information within its computer systems) on how to adequately protect Private Information.

109. Defendant owed a duty to Plaintiff and the Class to implement processes that would detect a breach on its data security systems in a timely manner.

110. Defendant owed a duty to Plaintiff and the Class to act upon data security warnings and alerts in a timely fashion.

111. Defendant owed a duty to Plaintiff and the Class to adequately train and supervise its employees to identify and avoid any phishing emails that make it past its email filtering service.

112. Defendant owed a duty to Plaintiff and the Class to disclose if its computer systems, software, and data security practices were inadequate to safeguard individuals' Private Information from theft because such an inadequacy would be a material fact in the decision to entrust Private Information with Defendant.

113. Defendant owed a duty to Plaintiff and the Class to disclose in a timely and accurate manner when data breaches occurred.

114. Defendant owed a duty of care to Plaintiff and the Class because they were foreseeable and probable victims of any inadequate data security practices.

E. Defendant was on Notice of Cyberattack Threats and of the Inadequacy of its Data Security.

115. Defendant was on notice that companies, including companies operating within and aiding the healthcare industry have been targets for cyberattacks.

116. Defendant was on notice that the FBI has recently been concerned about data security in the healthcare industry. In August 2014, after a cyberattack on Community Health Systems, Inc., the FBI warned companies within the healthcare industry that hackers were targeting them. The warning stated that "[t]he FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining the Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII)."[21]

117. The American Medical Association ("AMA") has also warned companies about the importance of protecting patients' confidential information:

> Cybersecurity is not just a technical issue; it's a patient safety issue. AMA research has revealed that 83% of physicians work in a practice that has experienced some kind of cyberattack. Unfortunately, practices are learning that cyberattacks not only threaten the privacy and security of patients' health and financial information, but also patient access to care.[22]

---

[21] Jim Finkle, *FBI Warns Healthcare Firms that they are Targeted by Hackers*, REUTERS (Aug. 2014), http://www.reuters.com/article/2014/08/20/us-cybersecurity-healthcare-fbi-idUSKBN0GK24U20140820.

[22] Andis Robeznieks, *Cybersecurity: Ransomware attacks shut down clinics, hospitals*, AM. MED. ASS'N (Oct. 4, 2019), https://www.ama-assn.org/practice-management/sustainability/cybersecurity-ransomeware-attacks-shut-down-clinics-hospitals.

118. Defendant was also on notice of the importance of data encryption of Private Information. Defendant knew it kept Private Information in its software and systems, yet it appears Defendant did not encrypt its software and systems, nor the information contained within them.

119. The United States Department of Health and Human Services' Office for Civil Rights urges the use of encryption of data containing sensitive personal information. As long ago as 2014, the Department fined two healthcare companies approximately two million dollars for failing to encrypt laptops containing sensitive personal information. In announcing the fines, Susan McAndrew, the DIBJI's Office of Human Rights' deputy director of health information privacy, stated "[o]ur message to these organizations is simple: encryption is your best defense against these incidents."[23]

120. As a company operating within the healthcare sector, and a covered entity or business associate under HIPAA, Defendant should have known about its data security weaknesses and sought better protection for the Private Information maintained on its systems and accumulating in its software.

F. Cybercriminals Will Use Plaintiff's and Class Members' Private Information to Defraud Them.

121. Plaintiff and Class Members' Private Information is of great value to hackers and cyber criminals, and the data stolen in the Data Breach will be used in a variety of

[23]"Stolen Laptops Lead to Important HIPAA Settlements," U.S. Dep't of Health and Human Services (Apr. 22, 2014), available at https://wayback.archive-it.org/3926/20170127085330/https://www.hhs.gov/about/news/2014/04/22/stolen-laptops-lead-to-important-hipaa-settlements.html.

sordid ways for criminals to exploit Plaintiff and Class Members and to profit off their misfortune.

122. Each year, identity theft causes tens of billions of dollars of losses to victims in the United States.[24] For example, with the Private Information stolen in the Data Breach, including Social Security numbers, identity thieves can open financial accounts, apply for credit, file fraudulent tax returns, commit crimes, create false driver's licenses and other forms of identification and sell them to other criminals or undocumented immigrants, steal government benefits, give breach victims' names to police during arrests, and many other harmful forms of identity theft.[25] These criminal activities have and will result in devastating financial and personal losses to Plaintiff and Class Members.

123. Private Information is such a valuable commodity to identity thieves that once it has been compromised, criminals will use it and trade the information on the cyber black-market for years.[26]

---

[24] "Facts + Statistics: Identity Theft and Cybercrime," Insurance Info. Inst., https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (discussing Javelin Strategy & Research's report "2018 Identity Fraud: Fraud Enters a New Era of Complexity").

[25] *See, e.g.*, Christine DiGangi, *5 Ways an Identity Thief Can Use Your Social Security Number*, Nov. 2, 2017, https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/.

[26] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO, July 5, 2007, https://www.gao.gov/assets/270/262904.htmlu.

124. For example, it is believed that certain Private Information compromised in the 2017 Experian data breach was being used, three years later, by identity thieves to apply for COVID-19-related benefits in the state of Oklahoma.[27]

125. This was a financially motivated Data Breach. "Once the attacker gains access to the target system, they proceed to encrypt valuable information, such as personal details, credit card information, or account credentials, which can fetch them monetary rewards…After encrypting the data, the threat actors demand a ransom to release the private key required for decryption. Ransoms are typically demanded in cryptocurrencies like Bitcoin or Ethereum, offering a degree of anonymity to the attackers. It is important to note that paying the ransom does not guarantee the release of the private key, and there is no guarantee that the cycle of attacks and ransom demands will cease."[28]

126. To date, there is no indication that Defendant has made any attempt to recover Plaintiff's and Class Members' Private Information.

127. The only reason cybercriminals go through the trouble of hacking companies like IBJI is to steal the highly sensitive information they maintain, which can be exploited and sold for use in the kinds of criminal activity described herein.

---

[27] *See* https://www.engadget.com/stolen-data-used-for-unemployment-fraud-ring-174618050.html; *see also* https://www.wired.com/story/nigerian-scammers-unemployment-system-scattered-canary/.

[28] https://www.encryptionconsulting.com/understanding-how-cybercriminals-hold-your-data-hostage/#:~:text=Modern%20ransomware%20employs%20hybrid%20encryption,private%20key%20required%20for%20decryption.

128. The Private Information exposed in this Data Breach is valuable to identity thieves for use in the kinds of criminal activity described herein.

129. These risks are both certainly impending and substantial. As the FTC has reported, if hackers get access to personally identifiable information, ***they will use it***.[29]

130. Hackers may not use the accessed information right away. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[30]

131. Medical-related identity theft is one of the most common, most expensive, and most difficult to prevent forms of identity theft. According to Kaiser Health News, "medical-related identity theft accounted for 43 percent of all identity thefts reported in the United States in 2013…," which is more than identity thefts involving banking and finance, the government and the military, or education.[31]

132. As indicated by James Trainor, second in command at the FBI's cyber security division: "Medical records are a gold mine for criminals—they can access a patient's name, DOB, Social Security and insurance numbers, and even financial

---

[29] Ari Lazarus, *How fast will identity thieves use stolen info?*, FED. TRADE COMM'N (May 24, 2017), https://www.consumer.ftc.gov/blog/2017/05/how-fast-will-identity-thieves-use-stolen-info.

[30] *See Cases Currently Under Investigation,* U.S. DEP'T OF HEALTH & HUMAN SERVS.: BREACH PORTAL, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.

[31] Michael Ollove, "The Rise of Medical Identity Theft in Healthcare," Kaiser Health News, Feb. 7, 2014, https://khn.org/news/rise-of-indentity-theft/.

information all in one place."[32] A complete identity theft kit that includes health insurance credentials may be worth up to $1,000 on the black market.[33]

133. When cybercriminals manage to steal health insurance information and other personally sensitive data—as they did here—there is no limit to the amount of fraud to which Plaintiff and Class Members are exposed.

134. "Hackers want stolen medical records to commit identity theft, use the stolen data as a ransom, sell it on the dark web or impersonate the victim to receive medical services. Medical records are valuable to cybercriminals as they allow cybercriminals to commit fraud and go undetected longer than they can with other Personally Identifiable Information[.]"[34]

135. "Unlike credit cards or login credentials, medical records have a long lifespan and cannot be easily altered making them valuable to cybercriminals. Stolen medical records are difficult for people to identify malicious activity with and allow cybercriminals to misuse them for longer periods undetected. Here are the ways cybercriminals use stolen medical records."[35]

---

[32] IDExperts, *You Got It, They Want It: Criminals Targeting Your Private Healthcare Data, New Ponemon Study Shows*, https://www.idexpertscorp.com/knowedge-center/single/you-got-it-they-want-it-criminals-are-targeting-your-private-healthcare-dat.

[33] *Managing cyber risks in an interconnected world*, PRICEWATERHOUSECOOPERS: Key findings from The Global State of Information Security Survey 2015, https://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf.

[34] https://www.keepersecurity.com/blog/2024/01/11/why-do-hackers-want-medical-records/#:~:text=Cybercriminals%20can%20commit%20crimes%20such,medical%20services%2C%20benefits%20and%20medications.

[35] *Id.*; https://www.hipaajournal.com/why-do-criminals-target-medical-records/.

136. "Healthcare records are so valuable because they can be used to commit a multitude of crimes. Social Security numbers, dates of birth, and demographic data can be used to commit identity theft to obtain loans and credit cards in victims' names. Healthcare data can be used to impersonate patients to obtain expensive medical services, Medicare and Medicaid benefits, healthcare devices, and prescription medications. Healthcare records also contain the necessary information to allow fraudulent tax returns to be filed to obtain rebates."[36]

137. "ID theft victims often have to spend money to fix problems related to having their data stolen, which averages $600 according to the FTC. But security research firm Ponemon Institute found that health care identity theft victims spend nearly $13,500 dealing with their hassles, which can include the cost of paying off fraudulent medical bills."[37]

138. As described above, identity theft victims must spend countless hours and large amounts of money repairing the impact to their credit.[38]

139. With this Data Breach, identity thieves have already started to prey on the victims, and one can reasonably anticipate this will continue.

[36] https://www.hipaajournal.com/why-do-criminals-target-medical-records/.
[37] https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/.
[38] "Guide for Assisting Identity Theft Victims," Federal Trade Commission, 4 (Sept. 2013), http://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-theft-victims.pdf.

140. Victims of the Data Breach, like Plaintiff and other Class Members, must spend many hours and large amounts of money protecting themselves from the current and future negative impacts to their credit because of the Data Breach.[39]

141. In fact, as a direct and proximate result of the Data Breach, Plaintiff and the Class have suffered, and have been placed at an imminent, immediate, and continuing increased risk of suffering, harm from fraud and identity theft. Plaintiff and the Class must now take the time and effort and spend the money to mitigate the actual and potential impact of the Data Breach on their everyday lives, including purchasing identity theft and credit monitoring services, placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, healthcare providers, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts, credit reports, and health insurance account information for unauthorized activity for years to come.

142. Plaintiff and the Class have suffered, and continue to suffer, actual harms for which they are entitled to compensation, including:

e. Trespass, damage to, and theft of their personal property including Private Information;

f. Improper disclosure of their Private Information;

g. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by their Private Information being placed in the hands of criminals and having been already misused;

[39] "Guide for Assisting Identity Theft Victims," Federal Trade Commission, 4 (Sept. 2013), http://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-theft-victims.pdf.

h. The imminent and certainly impending risk of having their Private Information used against them by spam callers to defraud them;

i. Damages flowing from Defendant' untimely and inadequate notification of the data breach;

j. Loss of privacy suffered as a result of the Data Breach;

k. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably expended to remedy or mitigate the effects of the data breach;

l. Ascertainable losses in the form of deprivation of the value of patients' personal information for which there is a well-established and quantifiable national and international market;

m. The loss of use of and access to their credit, accounts, and/or funds;

n. Damage to their credit due to fraudulent use of their Private Information; and/or

o. Increased cost of borrowing, insurance, deposits and other items which are adversely affected by a reduced credit score.

143. Moreover, Plaintiff and Class Members have an interest in ensuring that their Private Information, which remains in the possession of Defendant, is protected from further breaches by the implementation of industry standard and statutorily compliant security measures and safeguards. Defendant has shown itself to be incapable of protecting Plaintiff's and Class Members' Private Information.

144. Plaintiff and Class Members are desperately trying to mitigate the damage that Defendant has caused them but, given the Private Information Defendant made accessible to cybercriminals, they are certain to incur additional damages. Because identity thieves have their Private Information, Plaintiff and all Class Members will need to have identity theft monitoring protection for the rest of their lives. Some may even need to go through the long and arduous process of getting a new Social Security number, with all the loss of credit and employment difficulties that come with this change.[40]

145. None of this should have happened. The Data Breach was entirely preventable.

G. IBJI Could Have Prevented the Data Breach but Failed to Adequately Protect Plaintiff's and Class Members' Private Information.

146. Data breaches are preventable.[41] As Lucy Thompson wrote in the DATA BREACH AND ENCRYPTION HANDBOOK, "[i]n almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions."[42] he added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised . . . ."[43]

---

[40] *Will a New Social Security Number Affect Your Credit?*, LEXINGTON LAW (Nov. 16, 2015), https://www.lexingtonlaw.com/blog/credit-101/will-a-new-social-security-number-affect-your-credit.html.
[41] Lucy L. Thompson, "Despite the Alarming Trends, Data Breaches Are Preventable," *in* DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012).
[42] *Id.* at 17.
[43] *Id.* at 28.

147. "Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures … Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a *data breach never occurs*."[44]

148. The FTC has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

149. In 2016, the FTC updated its publication, *Protecting Private Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[45]

150. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex

[44] *Id.*

[45] *Protecting Private Information: A Guide for Business*, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

151. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

152. These FTC enforcement actions include actions against healthcare providers and partners like Defendant. *See, e.g., In the Matter of Labmd, Inc., A Corp*, 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.").

153. Defendant failed to properly implement basic data security practices, including those set forth by the FTC.

154. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to customers' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

155. Defendant also failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-

5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

156. Defendant required Plaintiff and Class Members to surrender their Private Information—including but not limited to their names, addresses, Social Security numbers, medical information, and health insurance information—and were entrusted with properly holding, safeguarding, and protecting against unlawful disclosure of such Private Information.

157. Many failures laid the groundwork for the success ("success" from a cybercriminal's viewpoint) of the Data Breach, starting with Defendant's failure to incur the costs necessary to implement adequate and reasonable cyber security procedures and protocols necessary to protect Plaintiff's and Class Members' Private Information.

158. Defendant was at all times fully aware of its obligation to protect the Private Information of Plaintiff and Class Members. Defendant was also aware of the significant repercussions that would result from its failure to do so.

159. Defendant maintained Plaintiff's and the Class's Private Information in a reckless manner. In particular, their Private Information was maintained and/or exchanged, unencrypted, in Defendant's systems and software which were maintained in a condition vulnerable to cyberattacks.

160. Defendant knew, or reasonably should have known, of the importance of safeguarding Private Information and of the foreseeable consequences that would occur if

Plaintiff's and Class Members' Private Information was stolen, including the significant costs that would be placed on Plaintiff and Class Members as a result of a breach.

161. The mechanism of the cyberattack and potential for improper disclosure of Plaintiff's and Class Members' Private Information was a known risk to Defendant, and thus Defendant was on notice that failing to take necessary steps to secure Plaintiff's and Class Members' Private Information from those risks left that information in a dangerous condition.

162. Defendant disregarded the rights of Plaintiff and Class Members by, *inter alia*, (i) intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure that its systems and software were protected against unauthorized intrusions; (ii) failing to disclose that it did not have adequately robust security protocols and training practices in place to adequately safeguard Plaintiff's and Class Members' Private Information; (iii) failing to take standard and reasonably available steps to prevent the Data Breach; (iv) concealing the existence and extent of the Data Breach for an unreasonable duration of time; and (v) failing to provide Plaintiff and Class Members prompt and accurate notice of the Data Breach.

V. CLASS ACTION ALLEGATIONS

163. Plaintiff incorporates by reference all allegations of the preceding paragraphs as though fully set forth herein.

164. Plaintiff brings all claims as class claims under Fed. R. Civ. P. ("Rule") 23. Plaintiff asserts all claims on behalf of the Nationwide Class, defined as follows:

Nationwide Class

All persons residing in the United States who were sent a Notice of Data Breach letter from Defendant or on Defendant's behalf.

165. Plaintiff reserves the right to amend the above definition(s) or to propose alternative or add subclasses in subsequent pleadings and motions for class certification.

166. **Numerosity:** The proposed Class is believed to be so numerous that the joinder of all members is impracticable. The proposed Subclass is also believed to be so numerous that joinder of all members would be impractical because it is comprised of over 180,000 individuals.

167. **Typicality:** Plaintiff's claims are typical of the claims of the Class. Plaintiff and all members of the Class were injured through Defendant's uniform misconduct. The same event and conduct that gave rise to Plaintiff's claims are identical to those that give rise to the claims of every other Class Member because Plaintiff and each member of the Class had their sensitive Private Information compromised in the same way by the same conduct of Defendant.

168. **Adequacy:** Plaintiff is an adequate representative of the Class because his interests do not conflict with the interests of the Class he seeks to represent; Plaintiff has retained counsel competent and highly experienced in data breach class action litigation; and Plaintiff and Plaintiff's counsel intend to prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiff and his counsel.

169. **Superiority:** A class action is superior to other available means of fair and efficient adjudication of the claims of Plaintiff and the Class. The injury suffered by each

individual Class Member is relatively small in comparison to the burden and expense of individual prosecution of complex and expensive litigation. It would be very difficult, if not impossible, for members of the Class individually to effectively redress Defendant's wrongdoing. Even if Class Members could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties, and to the court system, presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties and provides benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

170. **Commonality and Predominance:** There are many questions of law and fact common to the claims of Plaintiff and other members of the Class, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the Class include:

a. Whether Defendant engaged in the wrongful conduct alleged herein;

b. Whether Defendant failed to adequately safeguard Plaintiff's and the Class's Private Information;

c. Whether Defendant's computer systems, software, and data security practices used to protect Plaintiff's and Class Members' Private Information violated the FTC Act, HIPAA, and/or state laws and/or Defendant' other duties discussed herein;

d. Whether Defendant owed a duty to Plaintiff and the Class to adequately protect their Private Information, and whether it breached this duty;

e. Whether Defendant knew or should have known that its computer and network security systems and business email accounts were vulnerable to a data breach;

f. Whether Defendant's conduct, including its failure to act, resulted in or was the proximate cause of the Data Breach;

g. Whether Defendant breached contractual duties owed to Plaintiff and the Class to use reasonable care in protecting their Private Information;

h. Whether Defendant failed to adequately respond to the Data Breach, including failing to investigate it diligently and notify affected individuals in the most expedient time possible and without unreasonable delay, and whether this caused damages to Plaintiff and the Class;

i. Whether Defendant continue to breach duties to Plaintiff and the Class;

j. Whether Plaintiff and the Class suffered injury as a proximate result of Defendant' negligent actions or failures to act;

k. Whether Plaintiff and the Class are entitled to recover damages, equitable relief, and other relief;

l. Whether injunctive relief is appropriate and, if so, what injunctive relief is necessary to redress the imminent and currently ongoing harm faced by Plaintiff and members of the Class and the general public;

m. Whether Defendant' actions alleged herein constitute gross negligence; and

n. Whether Plaintiff and Class Members are entitled to punitive damages.

VI. CAUSES OF ACTION

COUNT ONE
NEGLIGENCE
(On Behalf of Plaintiff and the Nationwide Class)

171. Plaintiff incorporates by reference the allegations in paragraphs 1–170 as though fully set forth herein.

172. Defendant solicited, gathered, and stored the Private Information of Plaintiff and the Class as part of the operation of its business.

173. Upon accepting and storing the Private Information of Plaintiff and Class Members, Defendant undertook and owed a duty to Plaintiff and Class Members to exercise reasonable care to secure and safeguard that information and to use secure methods and to implement necessary data security protocols and employee training to do so.

174. Defendant had full knowledge of the sensitivity of the Private Information, the types of harm that Plaintiff and Class Members could and would suffer if the Private Information was wrongfully disclosed, and the importance of adequate security.

175. Plaintiff and Class Members were the foreseeable victims of any inadequate safety and security practices. Plaintiff and the Class Members had no ability to protect their Private Information that was in Defendant' possession. As such, a special relationship existed between Defendant and Plaintiff and the Class.

176. Defendant owed Plaintiff and Class Members a common law duty to use reasonable care to avoid causing foreseeable risk of harm to Plaintiff and the Class when obtaining, storing, using, and managing their Private Information, including taking action to reasonably safeguard such data and providing notification to Plaintiff and the Class Members of any breach in a timely manner so that appropriate action could be taken to minimize losses.

177. Defendant's duty extended to protecting Plaintiff and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. See Restatement (Second) of Torts § 302B. Numerous courts and legislatures have also recognized the existence of a specific duty to reasonably safeguard personal information.

178. Defendant had duties to protect and safeguard the Private Information of Plaintiff and the Class from being vulnerable to compromise by taking common-sense precautions when dealing with sensitive Private Information. Additional duties that Defendant owed Plaintiff and the Class include:

a) To exercise reasonable care in designing, implementing, maintaining, monitoring, and testing Defendant' networks, systems, protocols, policies, procedures and practices to ensure that Plaintiff's and Class Members' Private Information was adequately secured from impermissible release, disclosure, and publication;

b) To protect Plaintiff's and Class Members' Private Information in its possession by using reasonable and adequate security procedures and systems; and

c) To promptly notify Plaintiff and Class Members of any breach, security incident, unauthorized disclosure, or intrusion that affected or may have affected their Private Information.

179. Only Defendant was in a position to ensure that its systems and protocols were sufficient to protect the Private Information that had been entrusted to them.

180. Defendant breached its duties of care by failing to adequately protect Plaintiff's and Class Members' Private Information. Defendant breached its duties by, among other things:

a) Failing to exercise reasonable care in obtaining, retaining, securing, safeguarding, protecting, and deleting the Private Information in its possession;

b) Failing to protect the Private Information in its possession using reasonable and adequate security procedures and systems;

c) Failing to train its employees as to how to detect and avoid phishing emails;

d) Failing to adequately and properly audit, test, and train its employees regarding how to properly and securely transmit and store Private Information;

e) Failing to adequately train its employees to not store unencrypted Private Information in their personal files longer than absolutely necessary for the specific purpose that it was sent or received;

f) Failing to consistently enforce security policies aimed at protecting Plaintiff's and the Class's Private Information;

g) Failing to mitigate the harm caused to Plaintiff and the Class Members;

h) Failing to implement processes to quickly detect data breaches, security incidents, or intrusions; and

i) Failing to promptly notify Plaintiff and Class Members of the Data Breach that affected their Private Information.

181. Defendant's willful failure to abide by these duties was wrongful, reckless, and grossly negligent in light of the foreseeable risks and known threats.

182. As a proximate and foreseeable result of Defendant's grossly negligent conduct, Plaintiff and the Class have suffered damages and are at imminent risk of additional harms and damages (as alleged above).

183. Through Defendant's acts and omissions described herein, including but not limited to Defendant's failure to protect the Private Information of Plaintiff and Class Members from being stolen and misused, Defendant unlawfully breached its duty to use

reasonable care to adequately protect and secure the Private Information of Plaintiff and Class Members while it was within Defendant's possession and control.

184. Further, through its failure to provide timely and clear notification of the Data Breach to Plaintiff and Class Members, Defendant prevented Plaintiff and Class Members from taking meaningful, proactive steps to securing their Private Information and mitigating damages.

185. As a result of the Data Breach, Plaintiff and Class Members have spent time, effort, and money to mitigate the actual and potential impact of the Data Breach on their lives, including but not limited to, paying for spyware removal, responding to the fraudulent use of the Private Information, and closely reviewing and monitoring bank accounts, credit reports, and statements sent from providers and their insurance companies.

186. Defendant's wrongful actions, inaction, and omissions constituted (and continue to constitute) common law negligence.

187. The damages Plaintiff and the Class have suffered (as alleged above) and will suffer were and are the direct and proximate result of Defendant's grossly negligent conduct.

188. Plaintiff and the Class have suffered injury and are entitled to actual and punitive damages in amounts to be proven at trial.

COUNT TWO
NEGLIGENCE PER SE
(On Behalf of Plaintiff and the Nationwide Class)

189. Plaintiff incorporates by reference the allegations in paragraphs 1–170 as though fully set forth herein.

190. Pursuant to the FTC Act, 15 U.S.C. § 45(a), Defendant had a duty to Plaintiff and the Class to provide fair and adequate computer systems and data security to safeguard the Private Information of Plaintiff and the Class.

191. Defendant is a covered entity under HIPAA, 45 C.F.R. §160.102, and as such is required to comply with the HIPAA's Privacy Rule and Security Rule. HIPAA requires Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). The confidential data at issue in this case constitutes "protected health information" within the meaning of HIPAA.

192. HIPAA further requires Defendant to disclose the unauthorized access and theft of the protected health information of Plaintiff and the Class "without unreasonable delay" so that Plaintiff and Class Members could take appropriate measures to mitigate damages, protect against adverse consequences, and thwart future misuse of their personal information. *See* 45 C.F.R. §§ 164.404, 164.406, and 164.410.

193. The FTC Act prohibits "unfair practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect Private Information. The FTC publications and orders described above also formed part of the basis of Defendant's duty in this regard.

194. Defendant gathered and stored the Private Information of Plaintiff and the Class as part of its business which affect commerce.

195. Defendant violated the FTC Act by failing to use reasonable measures to protect the Private Information of Plaintiff and the Class and by not complying with applicable industry standards, as described herein.

196. Defendant breached its duties to Plaintiff and the Class under the FTC Act and HIPAA by failing to provide fair, reasonable, or adequate computer systems and/or data security practices to safeguard Plaintiff's and Class Members' Private Information, and by failing to provide prompt notice without reasonable delay.

197. Defendant's multiple failures to comply with applicable laws and regulations constitutes negligence *per se*.

198. Plaintiff and the Class are within the class of persons that HIPAA and the FTC Act were intended to protect.

199. The harm that occurred as a result of the Data Breach is the type of harm HIPAA and the FTC Act were intended to guard against.

200. Defendant breached its duties to Plaintiff and the Class under these laws by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and the Class's Private Information.

201. Additionally, Defendant had a duty to promptly notify Plaintiff and the Class of the Data Breach. For instance, HIPAA required Defendant to notify victims of the Breach within 60 days of the discovery of the Data Breach. Defendant did not begin sending Notice of Data Breach Letters to Plaintiff and Class Members until on or around May 2024, despite knowing on or before June 2023 that unauthorized persons had accessed

and/or acquired their Private Information. Plaintiff and Class Members received the Notice of Data Breach Letters after the 60-day period proscribed by HIPAA.

202. Defendant breached its duties to Plaintiff and the Class by unreasonably delaying and failing to provide notice of the Data Breach expeditiously and/or as soon as practicable to Plaintiff and the Class.

203. Defendant's violation of the FTC Act and HIPAA constitutes negligence *per se*.

204. As a direct and proximate result of Defendant' negligence *per se*, Plaintiff and the Class have suffered, and continue to suffer, damages arising from the Data Breach, as alleged above.

205. The injury and harm that Plaintiff and Class Members suffered (as alleged above) was the direct and proximate result of Defendant's negligence *per se*.

206. Plaintiff and the Class have suffered injury and are entitled to damages in amounts to be proven at trial.

COUNT THREE
INVASION OF PRIVACY (INTRUSION UPON SECLUSION)
(On Behalf of Plaintiff and the Nationwide Class)

207. Plaintiff incorporates by reference the allegations in paragraphs 1–170 as though fully set forth herein.

208. Plaintiff and Class Members reasonably expected that the sensitive Private Information entrusted to Defendant would be kept private and secure and would not be disclosed to any unauthorized third party or for any improper purpose.

209. Defendant unlawfully invaded the privacy rights of Plaintiff and Class Members by:

a) Failing to adequately secure their sensitive Private Information from disclosure to unauthorized third parties or for improper purposes;

b) Enabling the disclosure of personal and sensitive facts and information about them in a manner highly offensive to a reasonable person; and

c) Enabling the disclosure of personal and sensitive facts about them without their informed, voluntary, affirmative, and clear consent.

210. A reasonable person would find it highly offensive that Defendant, having collected Plaintiff's and Class Members' sensitive Private Information, failed to protect such Private Information from unauthorized disclosure to third parties.

211. In failing to adequately protect Plaintiff's and Class Members' sensitive Private Information, Defendant acted in reckless disregard of their privacy rights. Defendant knew or should have known that its ineffective security measures, and the foreseeable consequences thereof, are highly offensive to a reasonable person in Plaintiff's and Class Members' position.

212. Defendant violated Plaintiff's and Class Members' right to privacy under the common law.

213. Defendant's unlawful invasions of privacy damaged Plaintiff and the Class. As a direct and proximate result of Defendant's unlawful invasion of privacy, Plaintiff and

Class Members suffered significant anxiety and distress, and their reasonable expectations of privacy were frustrated and defeated. Plaintiff and the Class seek actual and nominal damages for these invasions of privacy.

COUNT FOUR
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Nationwide Class)

214. Plaintiff incorporates by reference the allegations in paragraphs 1–170 as though fully set forth herein.

215. Plaintiff and the Class bring this claim in the alternative to all other claims and remedies at law.

216. Through the use of Defendant's services, Defendant received monetary benefits from Plaintiff and the Class.

217. Defendant collected, maintained, and stored the Private Information of Plaintiff and Class Members and, as such, Defendant had direct knowledge of the monetary benefits conferred upon it.

218. Defendant, by way of its affirmative actions and omissions, including its knowing violations of its express or implied contracts with Plaintiff and the Class Members, knowingly and deliberately enriched itself by saving the costs it reasonably and contractually should have expended on HIPAA compliance and reasonable data privacy and security measures to secure Plaintiff's and Class Members' Private Information.

219. Instead of providing a reasonable level of security, training, and protocols that would have prevented the Data Breach, as described above and as is common industry practice among companies entrusted with similar Private Information, Defendant, upon

information and belief, instead consciously and opportunistically calculated to increase its own profits at the expense of Plaintiff and Class Members.

220. As a direct and proximate result of Defendant's decision to profit rather than provide adequate data security, Plaintiff and Class Members suffered and continue to suffer actual damages, including (i) the amount of the savings and costs Defendant reasonably and contractually should have expended on data security measures to secure Plaintiff's Private Information, (ii) time and expenses mitigating harms, (iii) diminished value of Private Information, (iv) loss of privacy, (v) harms as a result of identity theft; and (vi) an increased risk of future identity theft.

221. Defendant, upon information and belief, has therefore engaged in opportunistic, unethical, and immoral conduct by profiting from conduct that it knew would create a significant and highly likely risk of substantial and certainly impending harm to Plaintiff and the Class in direct violation of Plaintiff's and Class Members' legally protected interests. As such, it would be inequitable, unconscionable, and unlawful to permit Defendant to retain the benefits it derived as a consequence of its wrongful conduct.

222. Accordingly, Plaintiff and the Class are entitled to relief in the form of restitution and disgorgement of all ill-gotten gains, which should be put into a common fund to be distributed to Plaintiff and the Class.

COUNT FIVE
BREACH OF IMPLIED CONTRACT
(On Behalf of the Nationwide Class)

223. Plaintiff incorporates by reference the allegations in paragraphs 1–170 as though fully set forth herein.

224. When Plaintiff and the Class members provided their Private Information to Defendant, they entered into implied contracts in which Defendant agreed to comply with its statutory and common law duties to protect Plaintiff's and Class members' Private Information and to timely notify them in the event of a data breach.

225. Defendant required Plaintiff and Class members to provide their Private Information in order for them to receive medical related services.

226. Based on the implicit understanding, Plaintiff and the Class accepted Defendant's offers and provided Defendant with their Private Information.

227. Plaintiff and Class members would not have provided their Private Information to Defendant had they known that Defendant would not safeguard their Private Information, as promised, or provide timely notice of a data breach.

228. Plaintiff and Class members fully performed their obligations under their implied contracts with Defendant.

229. Defendant breached the implied contracts by failing to safeguard Plaintiff's and Class members' Private Information and by failing to provide them with timely and accurate notice of the Data Breach.

230. The losses and damages Plaintiff and Class members sustained (as described above) were the direct and proximate result of Defendant' breach of their implied contracts with Plaintiff and Class members.

COUNT SIX
BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiff and the Nationwide Class)

231. Plaintiff incorporates by reference the allegations in paragraphs 1–170 as though fully set forth herein.

232. In light of the special relationship between Defendant and Plaintiff and Class Members, whereby Defendant became guardian of Plaintiff's and Class Members' Private Information, Defendant became a fiduciary by its undertaking and guardianship of the Private Information, (i) to act primarily for Plaintiff and Class Members, (ii) for the safeguarding of their Private Information; (iii) to timely notify Plaintiff and Class Members of a data breach's occurrence and disclosure; and (iv) to maintain complete and accurate records of what information (and where) Defendant did and does store.

233. Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of Defendant's relationship with its clients' patients, in particular, to keep secure their Private Information.

234. Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class Members because of the high degree of trust and confidence inherent to the nature of the relationship between Plaintiff and Class Members on the one hand and Defendant on the other, including with respect to their Private Information.

235. Defendant breached its fiduciary duties to Plaintiff and Class Members by failing to diligently discover, investigate, and give notice of the Data Breach in a reasonable and practicable period of time.

236. Defendant breached its fiduciary duties to Plaintiff and Class Members by failing to encrypt and otherwise protect the integrity of the systems containing Plaintiff's and Class Members' Private Information.

237. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to timely notify and/or warn Plaintiff and Class Members of the Data Breach.

238. Defendant breached its fiduciary duties to Plaintiff and Class Members by otherwise failing to safeguard Plaintiff's and Class Members' Private Information.

239. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) theft of their Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information.

COUNT SEVEN
DECLARATORY AND INJUNCTIVE RELIEF
(On Behalf of Plaintiff and the Nationwide Class)

240. Plaintiff incorporates by reference the allegations in paragraphs 1–170 as though fully set forth herein.

241. This count is brought under the Federal Declaratory Judgment Act, 28 U.S.C. § 2201.

242. As previously alleged, Defendant was required to provide adequate security for the Private Information collected from Plaintiff and the Class.

243. Defendant owed and still owes a duty of care to Plaintiff and Class Members that require them to adequately secure Plaintiff's and Class Members' Private Information.

244. Upon reason and belief, Defendant still possesses the Private Information of Plaintiff and the Class Members.

245. Defendant has not satisfied its contractual obligations and legal duties to Plaintiff and the Class Members.

246. Since the Data Breach, Defendant has not yet announced any changes to its data security infrastructure, processes, or procedures to fix the vulnerabilities in its computer systems and/or security practices which permitted the Data Breach to occur and go undetected and, thereby, prevent further attacks.

247. Defendant has not satisfied its contractual obligations and legal duties to Plaintiff and the Class. In fact, now that Defendant's insufficient data security is known to hackers, the Private Information in Defendant's possession is even more vulnerable to cyberattack.

248. Actual harm has arisen in the wake of the Data Breach regarding Defendant's contractual obligations and duties of care to provide security measures to Plaintiff and the members of the Class. Further, Plaintiff and the members of the Class are at risk of additional or further harm due to the exposure of their Private Information and Defendant's failure to address the security failings that led to such exposure.

249. There is no reason to believe that Defendant's data security measures are any more adequate now than they were before the Data Breach to meet Defendant's contractual obligations and legal duties.

250. Plaintiff and the Class, therefore, seek a declaration (i) that Defendant's existing security measures do not comply with its contractual obligations and duties of care to provide adequate security, and (ii) that to comply with its contractual obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to:

a) Ordering Defendant engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

b) Ordering Defendant engage third-party security auditors and internal personnel to run automated security monitoring;

c) Ordering Defendant audit, test, and train its security personnel regarding any new or modified procedures;

d) Ordering Defendant segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's systems is compromised, hackers cannot gain access to other portions of Defendant's systems;

e) Ordering Defendant purge, delete, and destroy, in a reasonably secure manner, customer data not necessary for their provisions of services;

f) Ordering Defendant conduct regular database scanning and security checks; and

g) Ordering Defendant routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach.

COUNT EIGHT
Violations of the Illinois Consumer Fraud and Deceptive Business Practices Act ("CFA"), 815 Ill. Comp. Stat. §§ 505/1, *et seq.*
(On Behalf of Plaintiff and the Nationwide Class)

251. Plaintiff incorporates by reference the allegations in paragraphs 1–170 as though fully set forth herein.

252. Plaintiff and the Class are "consumers" as defined in 815 Ill. Comp. Stat. § 505/1(e). Plaintiff, the Class, and Defendant are "persons" as defined in 815 Ill. Comp. Stat. § 505/1(c).

253. Defendant engaged in "trade" or "commerce," including the provision of services, as defined under 815 Ill. Comp. Stat. § 505/1(f). Defendant engages in the sale of "merchandise" (including services) as defined by 815 Ill. Comp. Stat. § 505/1(b) and (d).

254. Defendant engaged in deceptive and unfair acts and practices, misrepresentation, and the concealment and omission of material facts in connection with the sale and advertisement of its services in violation of the CFA, including: (i) failing to maintain adequate data security to keep Plaintiff's and the Class Members' sensitive PII from being stolen by cybercriminals and failing to comply with applicable state and federal laws and industry standards pertaining to data security, including the FTC Act; (ii) failing to disclose or omitting materials facts regarding their lack of adequate data security and inability or unwillingness to properly secure and protect the PII of Plaintiff and the Class; (iii) failing to disclose or omitting materials facts about Defendant's failure to comply with the requirements of relevant federal and state laws pertaining to the privacy and security of the PII of Plaintiff and the Class; and (iv) failing to take proper action following the Data Breach to enact adequate privacy and security measures and protect Plaintiff' and the Class's PII and other PII from further unauthorized disclosure, release, data breaches, and theft.

255. These actions also constitute deceptive and unfair acts or practices because Defendant knew the facts about their inadequate data security and failure to comply with applicable state and federal laws and industry standards would be unknown to and not easily discoverable by Plaintiff and the Class and defeat their reasonable expectations about the security of their PII.

256. Defendant intended reliance on its deceptive and unfair acts and practices and the concealment and omission of material facts in connection with Defendant's goods and services.

257. Defendant's wrongful practices were and are injurious to the public because those practices were part of Defendant's generalized course of conduct that applied to the Class. Plaintiff and the Class have been adversely affected by Defendant's conduct and the public was and is at risk as a result thereof.

258. Defendant also violated 815 ILCS 505/2 by failing to immediately notify Plaintiff and the Class of the nature and extent of the Data Breach pursuant to the Illinois PII Protection Act, 815 ILCS 530/1, *et seq*.

259. As a result of Defendant's wrongful conduct, Plaintiff and the Class were injured in that they never would have allowed their PII to be provided to Defendant had they known or been told that Defendant failed to maintain sufficient security to keep their PII from being hacked and taken and misused by others.

260. As a direct and proximate result of Defendant's violations of the CFA, Plaintiff and the Class have suffered harm: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fail to undertake appropriate and adequate measures to protect PII in their continued possession; and/or (vii) future costs in

terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

261. Pursuant to 815 Ill. Comp. Stat. § 505/10a(a), Plaintiff and the Class seek actual and compensatory damages, injunctive relief, and court costs and attorneys' fees because of Defendant's violations of the CFA.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiff and the Class pray for judgment against Defendant as follows:

a. An order certifying this action as a class action under Rule 23, defining the Class as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiff is a proper representative of the Class requested herein;

b. A judgment in favor of Plaintiff and the Class awarding them appropriate monetary relief, including actual damages, restitution, attorney fees, expenses, costs, and such other and further relief as is just and proper.

c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class and the general public as requested herein, including, but not limited to:

i. Ordering that Defendant engage third-party security auditors/penetration testers as well as internal security

personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant' systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

ii. Ordering that Defendant engage third-party security auditors and internal personnel to run automated security monitoring;

iii. Ordering that Defendant audit, test, and train their security personnel regarding any new or modified procedures;

iv. Ordering that Defendant segment customer data by, among other things, creating firewalls and access controls so that if one area of Defendant' systems is compromised, hackers cannot gain access to other portions of Defendant' systems;

v. Ordering that Defendant cease transmitting Private Information via unencrypted email;

vi. Ordering that Defendant cease storing Private Information in email accounts;

vii. Ordering that Defendant purge, delete, and destroy in a reasonably secure manner customer data not necessary for its provisions of services;

viii. Ordering that Defendant conduct regular database scanning and securing checks;

ix. Ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

x. Ordering Defendant to meaningfully educate current, former, and prospective employees and subcontractors about the threats faced as a result of the loss of financial and personal information to third parties, as well as the steps they must take to protect against such occurrences;

d. An order requiring Defendant to pay the costs involved in notifying the Class Members about the judgment and administering the claims process;

e. A judgment in favor of Plaintiff and the Class awarding them pre-judgment and post-judgment interest, reasonable attorneys' fees, costs and expenses as allowable by law; and

f. An award of such other and further relief as this Court may deem just and proper.

VIII. DEMAND FOR JURY TRIAL

Plaintiff hereby demands a trial by jury on all appropriate issues raised in this Class Action Complaint.

Date: September 16, 2024

Respectfully submitted,

/s/: William B. Federman

William B. Federman
FEDERMAN & SHERWOOD
10205 N. Pennsylvania Ave.
Oklahoma City, OK 73120
T: (405) 235-1560
F: (405) 239-2112
E: wbf@federmanlaw.com